UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/912,403	07/26/2001	William Michael Raike	P65847US1	4247

7590 03/06/2006

JACOBSON HOLMAN
PROFESIONAL LIMITED LIABILITY COMPANY
400 SEVENTH STREET, N.W.
WASHINGTON, DC 20004

EXAMINER	
NGUYEN, MINH DIEU T	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 03/06/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/912,403	RAIKE, WILLIAM MICHAEL	
	Examiner	Art Unit	
	Minh Dieu Nguyen	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) *1 and 6-8* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-5 and 9-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on December 5, 2005 has been entered.

2. This office action is in response to the communication dated December 5, 2005 with the amendments to claims 2-5, the cancellation of claims 1 and 6-8 and the addition of claims 9-16.

3. Claims 2-5 and 9-16 are pending.

Response to Arguments

4. Applicant's arguments filed December 5, 2005 have been fully considered but they are not persuasive.

5. Applicant argues that the interpretation of the packet ID (PID) described in Wasilewski is incorrect.

The examiner disagrees, from the specification (col. 6 lines 47-57) and the drawings (Fig. 3A, 3B and 4), Wasilewski specifically discloses assigning a unique packet ID and inserting the unique packet ID in a header section of each transport packet. It clearly reads on unique packet tag assigned to each data packet (claims 9 and 13).

6. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., "the packet ID are not unique at the packet level as required by the present claims") are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Claim Rejections - 35 USC § 112

7. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

8. Claims 9 and 13 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Claim 9 states transmitting the packet key, the base key to a recipient, there is no support for this limitation in the specification and drawing. The packet key is used to encrypt data packet, it should not be transmitted in the clear to the recipient, and the base key is encrypted before transmitting to the recipient according to the specification (page 3, lines 20-23). Claim 13 states computing a packet key

based on the encrypted base key, there is no support for this limitation in the specification and drawing, according to the specification (page 2, lines 13-14; Fig. 1) the packet key is recreated by computing a secure hash of the base key.

9. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claims 5 and 16 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

11. Claims 5 and 16 recite the limitation "the group". There is insufficient antecedent basis for this limitation in the claim.

Specification

12. The disclosure is objected to because of the following informalities:

On page 4, line 26, "to encrypt the packet key" should be changed to "to encrypt the base key" according to the Fig. 1.

Appropriate correction is required.

13. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: the specification is not clear on how the packet key and the base key are transmitted to a recipient (claim 9) and computing a packet key for each packet based on the encrypted base key (claim 13).

Claim Rejections - 35 USC § 103

14. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

15. Claims 4-5 and 9, 11, 13 and 15-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski (5,420,866) in view of Bleichenbacher et al. (6,735,313) and further in view of Levy et al (6,212,633).

a) As to claims 9, 11, 13 and 15, as best understood, Wasilewski discloses methods for providing conditional access information to decoders in a packet-based multiplexed communications system comprising a transmitter (Fig. 2, element 198) encrypts payload sections of each transport packet stream of data (col. 9, lines 30-36) that assigned a unique packet ID (PID) (col. 8, lines 44-46) using unique encryption control words (col. 9, lines 26-30); transmitter adds the packet ID to the corresponding encrypted packet data; inserts the packet so processed into the packet stream and transmit the encrypted data packet stream, unique packet ID and the packet key to the recipient (Figs. 3A and 3B; col. 9, lines 45-47). Wasilewski also discloses at the recipient's station (Fig. 2, element 201), each received encrypted packet is decrypted by the decryption information respective to each packet ID (Fig. 6; col. 14, lines 13-20) and the decrypted packet data is outputted in a form suitable for playing the streamed media (Fig. 2, element 208).

Wasilewski does not specifically disclose the encryption key (i.e. packet key) used for encrypting packet data is being based on the random base key and the assigned tag value of the packet.

Bleichenbacher discloses a system for transmitting an encrypted program together with a program identifier which is used by a set top terminal, together with stored entitlement information, to derive the decryption key necessary to decrypt the program (col. 1, lines 9-15), the system comprising a program key used to encrypt each program (col. 3, lines 4-6), the program key is created by applying a hash function to the master key and program identifier (col. 3, lines 30-37). The master key which reads on the base key may be updated for security reason (col. 7, lines 21-23). Bleichenbacher also discloses the decryption process (Fig. 9).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ creating a packet key based on a base key and a unique packet tag assigned to each data packet in the system of Wasilewski as Bleichenbacher discloses so as to enhance security of key and data against hackers.

b) As to claim 4, Wasilewski, as modified above, discloses the packet data is encrypted using a symmetric encryption algorithm in conjunction with the packet key and the encrypted data is decrypted at the recipient's station using the symmetric encryption algorithm in conjunction with the recreated packet key (col. 3, line 45 to col. 4, line 6).

c) As to claims 5 and 16, Bleichenbacher, as modified above, discloses the hash function used to create and reestablish the packet key is SHA-1 or MD5 (col. 5, lines 43-47).

16. Claims 3, 10, 12 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski (5,420,866) in view of Bleichenbacher et al. (6,735,313) and further in view of Levy et al (6,212,633).

Both Wasilewski and Bleichenbacher do not specifically disclose encrypting the random base key using a public key encryption algorithm to create an open key prior to transmission.

Levy discloses a secure data communication incorporating data encryption and/or access control comprising the steps of generating randomly a session key, encrypting the session key (col. 13, line 64 to col. 14, line 3) and transmit the encrypted session key to target node (col. 14, lines 15-17).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of encrypting the base key using a public key encryption algorithm as Levy teaches in the system of Wasilewski and Bleichenbacher so as to enhance the security of transmitted information.

17. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski (5,420,866) in view of Bleichenbacher et al. (6,735,313) in view of Levy et al (6,212,633) and further in view of Hawthorne (5,768,381).

Wasilewski, Bleichenbacher and Levy do not specifically disclose transmitting the open key by adding it to a header of the transmission.

Hawthorne discloses encryption and decryption of electronically transmitted messages (col. 1, lines 6-10) comprising transmitting encrypted session key (i.e. open key) as header to the recipient.

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of transmitting the open key to the recipient by adding it to the stream header in the system of Wasilewski, Bleichenbacher and Levy as Hawthorne teaches so as to strengthen secure communications between two entities.

Conclusion

18. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

mdn
3/1/06

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER